Docket No.:  1083.1048

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re the Application of:

Takayuki HASEBE et al.

Serial No. 09/000,924                                    Group Art Unit: 2165

Confirmation No.

Filed: December 30, 1997                                 Examiner:  Nguyen, C.

For:    DATA PROTECTION SYSTEM, DATA PREPARATION DEVICE, AND DATA WORKING
        DEVICE

**INFORMAL**

**AGENDA FOR EXAMINER INTERVIEW ONLY**

The Applicants respectfully request consideration of the claim amendments submitted in
the Amendment filed December 4, 2000.  Recitation of pending claims is attached for reference
convenience.

In the Office Action mailed July 17, 2001, the Examiner rejected claims 1-18, 20, and 22-
23 under 35 USC 103 as being unpatentable over Hasebe #1 (US Patent No. 5,392,351) in view
of Hasebe #2 (US Patent No. 5,761,651) and further in view of Iwayama (US Patent No.
5,832,083).

**PRIOR ART**

**Hasebe #1**

Hasebe #1 discloses a data protection system for preventing unauthorized copying of
electronic data, such as computer software (Hasebe #1 at abstract, Col. 1, lines 6 - 9).  The
protected software is provided to the user encrypted on a storage medium such as an optical
disk (Col. 1, lines 63 - 65; Col. 2, lines 27 - 29).  The electronic key for decrypting the data is
stored on the storage medium in encrypted form (Col. 1, line 66 - Col. 2, line 3).  The vendor
computer supplies encrypted permission information, for decrypting the encrypted electronic
data, to the user computer via transmission or to the user in a document (Col. 2, lines 14 - 26).
Upon decryption, the unencrypted software is available for execution by the user (Col. 3, lines 37
- 39; Col. 5, line 66 - Col. 6, line 2).

### Hasebe #2

Hasebe #2 discloses a system for charging for use of digitized data such as software and for granting permission to use the data (Hasebe #2 at abstract; Col. 1, lines 7 - 9). The supplied data is decrypted for use by a software managing module (Col. 3, lines 46 - 65). Deciphering for subsequent use by the user is permitted only if an available credit balance exists in a charging table (Col. 4, lines 18 - 21). The available balance is subtracted based on the deciphering processing amount or the processing period of time for the ciphered software data (Col. 4, lines 23 - 25). The user can add to the remaining balance total to permit additional use of the data (Col. 4, lines 25 - 29).

### Iwayama

Iwayama et al. discloses a system for authorized accessing of encoded electronic data such as computer software (Iwayama et al. at abstract; Col. 2, lines 11 - 15). The data is first stored as encoded data on a storage medium such as a compact disk (Col. 2, lines 30 - 33). The desired portion of encoded data will be decoded when a user inputs the identification information for the preferred data content (Col. 2, lines 61 - 65). When the decoding is completed, the system compares the decoded content identification information with the user-supplied content information (Col. 3, lines 14 - 19). If the two sets of information match, the system will output the selected data portion to the user (Col. 3, lines 19 - 22).

## DISTINCTIONS OF THE PRESENT INVENTION OVER THE PRIOR ART

### Examiners' Assertions:

The Examiner appears to acknowledge that none of the relied upon references disclose about means for forbidding saving <u>input data</u> which requires authorization for use. Page 11 of the Action. The Examiner appears to assert that this feature would be obvious to one of ordinary skill in the art. However, the relied upon references do not suggest a motivation to prevent storage of <u>input data</u> which requires authorization for use (emphasis added). In particular, <u>input data</u> is data input when preparing data, such as data linked in a document when creating a compound document.

The Applicants respectfully assert that the claimed present invention as recited, for example, in claim 1 is not obvious. Claim 1 recites "<u>preventing storage of *the input data* linked in the appended compound data</u>" so as "to prevent <u>unauthorized use of the input data linked in the appended compound data</u> if the input data linked in the appended compound data <u>is judged to require authorization for use</u> (emphasis added). The term "compound data" means a

2

document that contains elements from different software applications. In particular, when displaying the document, an element in the document can be manipulated by the application that created the element. *See* page 2, lines 17-20 of the present application.

In contrast to the relied upon references, the claimed present invention prevents unauthorized use of input data, such as linked data in a compound document. Fig. 5 shows a system in which conventional programming techniques can be used, such as the Object Linking and Embedding (OLE) compound document standard. According to the present invention, link information can show which data (file) is linked based on the standard techniques of the OLE and then the boxes in Fig. 4 can judge whether the linked data requires authorization. Of course, in the present invention the link information is used to judge whether the linked data in a compound document requires authorization. Therefore, the present invention can perform the judgment if the link information specifying the linked data is at least specified. However, the present invention can also use information attached to the link information to judge whether the linked data requires authorization. *See* Figs. 2, 5 and 4 and on page 13, line 24 through page 14, line 9 of the present Application. *See also,* page 14, line 10 through page 16, line 6.

Independent claim 1, 4, 9, 18, 22 and 23:

In contrast to the relied upon references, the present invention (as recited in independent claims 1, 22 and 23, using the recitation of claim 1 as an example) provides "means for preventing storage of the input data linked in the appended compound data in another storage means to prevent unauthorized use of the input data linked in the appended compound data if the input data linked in the appended compound data is judged to require authorization for use" (emphasis added).

Independent claims 4 and 9:

In contrast to the relied upon references, the present invention (as recited in independent claims 4, 9, 15 and 20, using the recitation of claim 4 as an example) provides

> means for preventing storage of the input data in another storage means during processing of the input data in the compound data when said input data has been judged to require authorization for use; and
>
> storage means for storing process information indicating what kind of processing has been performed on the input data in the compound data during the processing (emphasis added).

### Independent claim 12:

In contrast to the relied upon references, the present invention as recited in independent claim 12, provides

A data preparation device wherein input data requiring authorization for use is input from a center which permits use of the input data in exchange for a charge, comprising:

X    means for creating compound data by linking input data, which requires authorization for use, in data;

means for generating information of the input data which is linked in the compound data;

means for appending the generated information to the compound data;

means for utilizing the compound data with the appended generated information by displaying the compound data, including displaying the input data (emphasis added).

### Independent claims 15 and 20:

In contrast to the relied upon references, the present invention (as recited in independent claims 15 and 20, using the recitation of claim 15 as an example) provides

X    means for processing input data, which requires authorization for use, and for creating compound data linking the input data in data; and

X    storage means for storing process information indicating what kind of processing has been applied by said processing means to the input data in the compound data (emphasis added).

### 35 USC 112, first paragraph, rejections

Claims 1-18, 20, and 22-23 were rejected under 35 USC 112, first paragraph. In particular, the Examiner appears to assert that the specification does not disclose computer program codes to enable one skilled in the art to make and use the invention. Therefore, the Examiner appears to assert that the specification does not include information about how a computer program performs the functions of the claimed present invention, for example, the boxes in Fig. 5 and the functions recited in claim 1. Page 9, item 16 of the Action.

OK    However, the Applicants assert that distinguishing features of the present invention do not concern actual programming techniques, so that computer program codes do not need to be provided for enablement.

4

For example, regarding claim 1 and Fig. 5, conventional programming techniques, such as the OLE standard, can be used to create a compound document with link information (Fig. 5, boxes 21, 22 and 23). The present invention can create the link information and add the link information to the compound document using the OLE programming techniques (box: link information generating unit 22 and link information appending unit 23). Once a compound document with the link information is created, upon use of the compound document, for example, display of the compound document, the system of the present invention uses conventional programming techniques to access the link information to determine if data in the compound document requires authorization (Fig. 4).

5